

CLAIMS

We claim:

1. A method for using a removable cryptographic module to enable a second device
5 to obtain secure access to encrypted compressed digital video content, comprising:
 - (a) receiving a rights enablement datum and a key derivation datum into said removable cryptographic module, where
 - (i) said rights enablement datum includes an encrypted representation of a key enabling decryption of said key derivation datum, and
 - 10 (ii) said key derivation datum includes an encrypted representation of a key enabling said second device to decrypt said encrypted content;
 - (b) said cryptographic module transforming said rights enablement datum, using a key stored in said cryptographic module, to determine said key enabling decryption of said key derivation datum;
 - 15 (c) said cryptographic module transforming said key derivation datum, using said key enabling decryption of said key derivation datum, to determine an initial content decryption key;
 - (d) said cryptographic module re-encrypting said initial content decryption key to produce a re-encrypted content decryption key datum, where:
 - 20 (i) said re-encrypted key datum enables said second device to decrypt said encrypted compressed digital video content, and
 - (ii) said re-encrypting is secured by a public key corresponding to said second device; and
 - (e) transmitting said re-encrypted content decryption key datum to said second
25 device.
2. The method of claim 1 where said re-encryption includes directly encrypting said initial content decryption key using said public key.
- 30 3. The method of claim 1 further comprising:
 - (i) said second device transforming said re-encrypted content decryption key datum to determine a key for decrypting said content; and
 - (ii) said second device decrypting said content.

4. The method of claim 3 further comprising said second device uncompressing said decrypted content.
- 5 5. The method of claim 3 where said transforming said re-encrypted content decryption key includes:
- (i) decrypting said re-encrypted content decryption key to recover said initial content decryption key;
 - (ii) computing an exclusive OR of (A) said initial content decryption key and (B) an additional secret parameter; and
 - 10 (iii) using a result of said exclusive OR operation as a key to decrypt said content.
6. The method of claim 5 where said removable cryptographic module is a smart card.
- 15 7. The method of claim 5 where said decrypting said re-encrypted key is performed using a RSA public key cryptosystem.
- 20 8. The method of claim 1 where said transforming said rights enablement datum includes using a symmetric block cipher to decrypt at least a portion of said rights enablement datum.
9. The method of claim 8 where said cryptographic module includes randomized hardware logic for a pseudoasymmetric transformation, and where said symmetric block cipher computation includes said randomized hardware transformation.
- 25 10. The method of claim 1 where said removable cryptographic module is a smart card.
- 30 11. A removable cryptographic device for enabling at least a second device to obtain secure access to encrypted compressed digital video content, comprising:
- (a) a nonvolatile memory;
 - (b) a key stored in said nonvolatile memory;

- (c) cryptographic logic configured to use said stored key to transform a rights enablement datum to determine a second key, where said second key enables decryption of a key derivation datum;
 - (d) cryptographic logic configured to use said second key to transform a key derivation datum to determine an initial content decryption key;
 - (e) cryptographic logic configured to re-encrypt said initial content decryption key in a manner secured using a public key corresponding to said second device; and
 - (f) an interface for communicating with said second device, configured to transmit said re-encrypted initial content decryption key to said second device.
12. The device of claim 11 configured as a smart card connectable to said second device.
13. The device of claim 12 where said second device includes:
- (i) an interface for receiving said encrypted compressed video content;
 - (ii) a smart card interface for communicating with said cryptographic device, configured to receive said re-encrypted initial content decryption key;
 - (iii) high-speed decryption logic configured to decrypt said content using a key derived from said re-encrypted initial content decryption key; and
 - (iv) video decompression logic configured to decompress said decrypted content.
14. The device of claim 13 where said decryption logic is configured to decrypt said content using a key computed as an exclusive OR of (A) a result of decrypting said re-encrypted initial content decryption key and (B) at least one additional secret parameter.
15. A removable cryptographic module enabling an associated device to obtain secure access to encrypted compressed digital video content, comprising:

- (a) means for receiving a rights enablement datum and a key derivation datum into said removable cryptographic module;
- (b) means for transforming said rights enablement datum, using a key stored in said cryptographic module, to determine a key enabling decryption of said key derivation datum;
- (c) means for transforming said key derivation datum, using said key enabling decryption of said key derivation datum, to determine an initial content decryption key;
- (d) means for re-encrypting said initial content decryption key to produce a re-encrypted content decryption key datum, where:
 - (i) said re-encrypted key datum enables said associated device to decrypt said encrypted compressed digital video content, and
 - (ii) said re-encrypting is secured by a public key corresponding to said associated device; and
- (e) means for transmitting said re-encrypted content decryption key datum to said associated device.

16. The removable cryptographic module of claim 15 where said means for re-encrypting includes means for directly encrypting said initial content decryption key using said public key.

17. The removable cryptographic module of claim 15 further comprising:

- (i) means, within said associated device, for transforming said re-encrypted content decryption key datum to determine a key for decrypting said content; and
- (ii) means, within said associated device, for decrypting said content.

18. The removable cryptographic module of claim 15 where said means for transforming said rights enablement datum includes means for using a symmetric block cipher to decrypt at least a portion of said rights enablement datum.

19. A removable cryptographic device for enabling at least one associated device to obtain secure access to encrypted compressed digital video content, comprising:

- (a) nonvolatile means for storing a key;

- (b) means for using said stored key to transform a rights enablement datum to determine a second key, where said second key enables decryption of a key derivation datum;
- (c) means for using said second key to transform a key derivation datum to determine an initial content decryption key;
- (e) means for re-encrypting said initial content decryption key in a manner secured using a public key corresponding to said associated device; and
- (f) means for transmitting said re-encrypted initial content decryption key to said associated device.

20. The device of claim 19 configured as a smart card connectable to said associated device.